Assessing the Army's Software Patch Management Process

Benjamin Alan Pryor

March 4, 2016

PUBLISHED BY
The Defense Acquisition University
Project Advisor: Jeff Caton
The Senior Service College Fellowship Program
Aberdeen Proving Ground, MD

Table of Contents

List of Figures

Note to Readers

The Strategy Research Project (SRP) is an integral part of the Senior Service College Fellowship (SSCF) program for the Department of Defense (DoD) Acquisition Community at the Aberdeen Proving Ground, Maryland, campus of Defense Acquisition University (DAU). Since the inception of the APG SSCF in 2009, the SRP implementation has emphasized the use of survey design and data collection. In January 2015, DoD Instruction 1100.13, *DoD Surveys*, was released and it included the requirement for DoD-level review of any "surveys requiring participation of personnel from more than one DoD or OSD component." Also, the implementation instructions for AR 335-14, *Management Information Control System*, added significant new review requirements for surveys. Changes driven by these new policies were not assessed at DAU before the start of APG SSCF Academic Year 2016.

Implementing the new review requirements could add 8 to 12 weeks to the SRP timeline and would not guarantee approval of any survey; such impacts cannot be reasonably accommodated within the existing SRP structure. Thus, the decision was made in December 2015 to remove the survey distribution and data collection from the SRP program and instead emphasize research based on evidence found in existing literature. Because this change was implemented in the middle of the APG SSCF 2015–2016 curriculum, the reader may detect minor impacts to the authors' research continuity that were beyond their ability to fully resolve.

Abstract

With the proliferation of information systems in the Department of Defense's inventory along with the rise of third-party software vulnerabilities, software patch management has become a key focus for the Department of Defense Cyber Command. The implementation of a software patch management plan is the first line of defense to protect the network from exploitation from cyberattacks. Three organizations are responsible for testing, integrating, and distributing software patches to the end-users: program management offices, the U.S. Army Software Engineering Command, and the Sustainment Automation Support Management Office (SASMO).

With the increasing rate of third-party software releases, the challenge facing the SASMO community is how to install these third-party software patches in the most expeditious and cost-effective manner. Nearly 15 years since the enactment of the Federal Information Security Management Act of 2002 as Public Law No. 107-347, many Federal agencies continue to report deficiencies in managing software patches within their systems. This study provides an overview of the software patch management process, an analysis of the reasons for the deficiencies in patch management, and some recommendations to assist the SASMO community to implement software patch management across the enterprise.

Chapter 1 – Introduction

Background

As the Army continues to field more tactical computers, keeping all of them updated with the current software patch to reduce system vulnerabilities is a daunting task, yet essential for network security. For the purpose of this research paper, a tactical information system is defined as an enterprise information system that performs specific functions such as financial, property book, supply, and medical management. According to Darcey (2003) "about 95% of all network intrusions could be avoided by keeping systems up to date with appropriate patches" (p. 5). A patch is defined as "an additional piece of code developed to address a problem in an existing piece of software" (Souppaya & Scarfone, 2013, p. vi).

The challenge in keeping these tactical information systems updated with the latest software version is that each of these systems operates a unique software configuration baseline and requires constant monitoring and installation of frequent software patch releases. To complicate matters more, many software patches cannot be automatically installed by the system administrators due to the unique software configurations. Before installing any software patches, they must be tested and integrated into the system software baseline by either the Program Management Office (PMO) or the United States Communications Electronics Command (CECOM) Software Engineering Center (SEC). This is to ensure that they do not negatively affect other software applications working in conjunction with the system.

In accordance with Department of the Army Pamphlet 70-3, *Army Acquisition Procedures*, the PMOs and CECOM SEC are responsible for releasing software updates for tactical information systems (Department of the Army, 2014). Since these two organizations are the gatekeepers for releasing and distributing software updates, the Army systems administrators

on the battlefield rely on them to provide the software patches. The timeline in which the systems administrators receive the software package varies from days to months depending on the complexity of the software and size of the update. The system administrators are prohibited from installing any unauthorized patch on these systems, as it may cause adverse effects. For example, installing a Microsoft Office patch may affect how the applications on the tactical system communicate with other applications within the system. Even with Cyber Command's initial bulk notification to their subordinate units of an available software security patch, also known as Information Assurance Vulnerability Alerts (IAVAs), system administrators in the field are prohibited from installing any software patch unless it is provided by the PMO or CECOM SEC (Department of the Army, 2013).

Unlike standard office automation computers that have a standard network-wide software baseline, tactical information systems do not have a standard software baseline. This nonstandard baseline causes a delay in the patching process. For standard office computers without a complex software baseline, a patch can be quickly tested, deployed, and automatically updated over the Defense Information Security Agency (DISA) Network Enterprise Centers (NECs) network. Conversely, the tactical information systems have a unique, complex software baseline that requires more time to test and integrate the patch into the system. Due to the sensitivity of most of the tactical system's application, most of the software patches cannot be installed automatically over the tactical Internet network (i.e., Very Small Aperture Terminals [VSATs]). In these instances, manual installation procedures must be performed. Another factor to consider is the size of the software patch and how it is released by the program manager (PM) or CECOM SEC. Given the size of the software patch, most of the system administrators receive it on a

media disc (e.g., CD or DVD) or they are directed to a secure Web site where they can download the patch individually for each respective system.

The Sustainment Automation Support Management Office (SASMO) is responsible for managing this network along with the tactical systems connected to it (Department of the Army, 2013). Although the VSAT device is linked directly into the DISA network, the NECs are not responsible for monitoring or managing the software baseline of tactical systems (Department of the Army, 2013). This delineation of responsibility is important, because the SASMOs must conduct network management without any assistance from outside agencies.

Problem Statement

How can the SASMO community maintain network security compliance on tactical systems when software patches are not readily available from the PMO or CECOM SEC? The SASMOs are responsible for managing the tactical network and the tactical information systems. Per Army Techniques Publication (ATP) 4-06.1, "SASMOs will not perform field level hardware (internal component) maintenance on tactical mission command systems and installation of patches on standard office automation. Personnel strength precludes operations extending into areas outside sustainment information systems support" (Department of the Army, 2013, p. 37). Their responsibility is to ensure their systems comply with the latest software security patches. A challenge for the SASMOs is that they are not responsible for developing, testing, or integrating the software patches into the software baseline. They are, on the other hand, responsible for installing the approved software patches onto the system. They depend on the PMOs and SEC to provide the software patch for installation onto the tactical computer. In order to reduce the likelihood of a network vulnerability, the SASMOs need to be given the most current software patch as soon as the vulnerability is disclosed by the third-party vendor.

Purpose of This Study

The purpose of this study is to determine whether Army Regulation (AR) 25-2 (Department of the Army, 2009) and ATP 4-0.6 need to be revised to support the software patch management process for tactical systems. Both of these references provide guidance and instructions on how to perform software patch management. AR 25-2 primarily focuses on the guidance to implement the software patch management process, while ATP 4-0.6 focuses on the implementation procedures for the SASMOs to follow for sustainment information systems with unique software baselines. The proliferation of sustainment information systems within the field, coupled with voluminous and frequent notification of third-party software patches, contributes to the growth of network vulnerabilities. Software updates need to be given to the SASMO community as soon as the vulnerability has been identified to ensure network integrity.

Based on the literature review, this research paper determines whether AR 25-2 needs to be modified to accelerate the receipt of software patches by tactical units in order to secure the network integrity. The literature review, in conjunction with the survey tool, addresses the notification process and receipt of the software patch by the SASMO community per ATP 4-0.6. The end state is to determine whether the software patch management process can be accelerated to achieve the Department of Defense (DoD) chief information officer's objective to "implement an automated patch management capability to distribute software and configuration patches, updates, and fixes to mitigate known, major vulnerabilities on DoD networks and systems against threats" (DoD, 2015b, p. 20).

Significance of This Research

With the proliferation of tactical information systems being fielded to the operational force and software vulnerability patches being released daily by third-party vendors, there is an

increased pressure on the PM and SEC to provide these software patches/updates to the field quickly. The current software patch management process is a slow and arduous procedure that exposes the network to adversaries (Government Accountability Office [GAO], 2004).

This research is relevant because software patches help secure the network by preventing network intrusion due to software vulnerabilities. The tactical systems are not alone in facing this challenge. Even the networks and systems within agencies are vulnerable to various types of intrusion and attack (DoD, 2015b, p. 10). In order to combat this growing concern of network vulnerabilities due to systems not being patched, the Army is starting to incorporate network security into their training programs. In 2015, the National Training Center at Fort Irwin, California, incorporated cybersecurity exercises into the training program. It has been reported that the Idaho National Guard was the first unit to receive a favorable assessment in deterring cyberattacks at the National Training Center (Meister, 2015). This type of event emphasizes the importance of software patch management in the operational force. These types of cyber-related training events are also being incorporated at the Joint Readiness Training Center in Louisiana. In a similar training event, Colonel Chuck Masaracchia, Armored Brigade commander, stated, "The greatest threat I face as a brigade commander on the battlefield is not [enemy] tanks, snipers or [improvised devices]… [but] defending the network" (Pomerleau, 2015).

The research determines whether the PMOs, SEC, and SASMO community have the essential tools and resources to accelerate the notification, delivery, and installation procedures of third-party software patches. Further research captures information regarding the SASMOs workforce to ensure they have the appropriate number of people to support the software patch management process. The findings may increase awareness of the strengths and/or shortcomings of each organization, which may lead to acceleration of the patch management process.

Overview of the Research Methodology

The data to support this research uses quantitative and qualitative information. The primary means of obtaining information was an online literature review primarily consisting of Army regulations and pamphlets, Army technical procedures, GAO reports, online defense articles, and academic papers. In addition to the literature review, a survey tool was used to capture quantitative data from the PMOs, CECOM SEC, and the SASMO community.

Research Questions

R1—How can the SASMO community accelerate the software patch management process once they receive the approved software patch?

R2—How can the PMO/SEC accelerate the software patch management process from their perspective?

Limitations

The research focused on Army tactical information systems supported by the SASMO community. This research did not focus on systems outside the purview of the tactical information systems, such as Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR); other PM-managed systems; and standard office automation systems on the garrison network.

One more limitation was the unavailability of information on how tactical systems manage the software patch process. Although there are many policies and regulations that address the software patch management process and the requirements to conduct periodic assessments on the systems, there are insufficient records on tactical systems. It is recommended that a study be done to determine whether a cyber command readiness inspection (CCRI) review should be incorporated at the tactical network level. A CCRI, which is conducted by DISA cyber

personnel, assesses the information assurance compliance of a unit’s tactical systems to ensure that patch management activities are being performed.

Chapter 2 – Literature Review

Information regarding the software patch management process for tactical systems was referenced in AR 25-2, ATP 4-0.6, online defense articles, GAO reports, and a DoD solicitation. There was limited information on the software patch management process for the tactical systems. Most of the information surrounding the subject focused on the standard office automation computers residing on the garrison network. Even with the limited information about the process on tactical systems, the literature did indicate DoD chief information officer (CIO) and Army awareness of software vulnerabilities on the tactical systems and the need for enhanced software security measures for the network. An anonymous chief weapon tester within the Pentagon stated in a defense media article, “Although the U.S. Department of Defense is making progress protecting its information and combat systems from cyberattacks, many vulnerabilities remain and more are expected to emerge” (Selinger, 2015).

The sections of this chapter provide background information highlighting reoccurring software security deficiencies found in various Federal agencies, policy and regulations on software patch management, Information Assurance Vulnerability Management (IAVM) Process, types of networks, and third-party vulnerabilities.

Policy and Regulations

Since 1997, GAO has designated information security as a severe risk (GAO, 2015a). In order to address this high-risk area, the Federal Information Security Management Act of 2002 (FISMA, 2002) was enacted as Title III of Public Law 107–347. The act established two requirements—information security program and evaluation requirements—for Federal agencies. This act was later updated with the Federal Information Security Modernization Act of 2014 (FISMA, 2014) to capture other growing security-related issues. The objective of FISMA 2002

and 2014 was for each agency to perform a self-assessment on their information security practices (GAO, 2015a, p. 2). To help assist the agencies, a Federal information security incident center, called the United States Computer Emergency Readiness Team, was established.

As part of the FIMSA 2014 requirement to report software security management control metrics to Congress, GAO (2015a) conducted an annual audit on 24 agencies from December 2014 to September 2015. The security deficiencies found within the report are separated into five categories, of which managing the configuration of software and hardware will be addressed in this section. Since 2003, the Office of Management and Budget (OMB) has instructed agency heads to provide an annual report of their information security metrics as part of the FISMA reporting requirements.

The GAO (2015a) report provides a 2013 and 2014 roll-up assessment of all the agencies' reporting requirements in each of the five categories. It publicized that 24 agencies continue to report deficiencies in five categories. These categories are access controls, configuration management controls, segregation of duties, contingency planning, and security management. Of these five major deficiency categories, only configuration management controls will be the focus of attention in the following section.

> The GAO (2015a) report describes configuration management control as
>
> … [ensuring] that only authorized and fully tested software is placed in operation, software and hardware is updated, information systems are monitored, patches are applied to these systems to protect against known vulnerabilities, and emergency changes are documented and approved. To protect against known vulnerabilities, effective procedures must be in place, current versions of vendor-supported software installed, and patches promptly implemented. Up-to-date patch

installation helps mitigate known flaws in software code that could be exploited to cause significant damage and enable malicious individuals to read, modify, or delete sensitive information or disrupt operations. (pp. 20–21)

Figure 1 provides a side-by-side comparison of the 24 agencies' information system controls audit manual control areas for 2013 and 2014. In 2014, 22 agencies stated deficiencies in the category of configuration management, which was slightly better than the previous year of 24 agencies. In addition to configuration management deficiencies, 22 agencies lacked control measures to release software to the end-users. Control measures guarantee that the system, both hardware and software, is monitored to ensure patches are up-to-date. For example, 17 of the 22 agencies reported various degrees of weaknesses in the timeliness of patch installation. The report further explains that one agency failed to apply high-risk updates to several of their systems. In addition to these findings, 14 agencies reported weaknesses in basic documentation procedures such as software configuration management. One agency lacked proper documentation for over 30 software configuration change approvals.

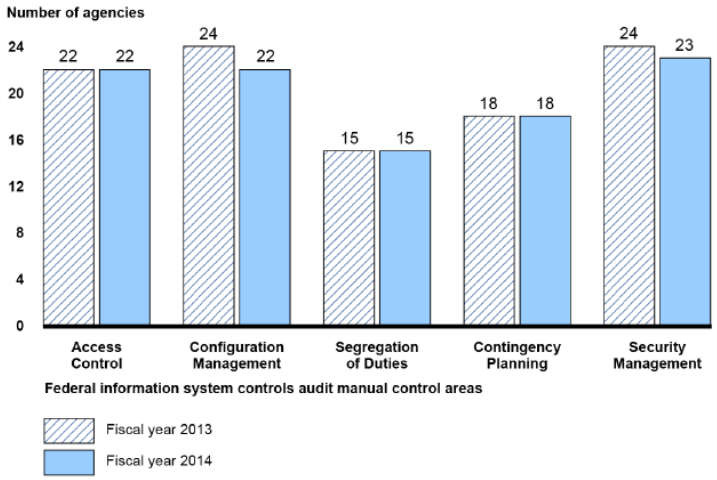


Figure 1 – Information Security Weakness at 24 Federal Agencies in FY 2013 and 2014
(Source: GAO, 2015a)

In another report, GAO (2015b) noted that the Internal Revenue Service had not installed software patches on their databases and servers. A similar finding appeared in a 2014 GAO report, which said that the Department of Veterans Affairs had yet to take appropriate action on addressing vulnerabilities identified in two key Web applications from 2011. Back in 2011, GAO reported that 21 agencies had problems with "maintaining and adhering to configuration management policies, plans, and procedures" (p. 14). The report continued by saying that many agencies had difficulty maintaining a detailed software baseline configuration. This issue leads into a discussion regarding personnel being properly trained.

Training

FISMA 2014 requires agencies to train and oversee personnel directly responsible for managing the security of the systems. In 2014, 22 of the 24 agencies conducted annual security awareness training for more than 90 percent of their network users, which was a decrease from 24 agencies in 2013 (GAO, 2015a). A similar downward trend can be seen in the establishment of a security awareness and training program. In 2014, 20 out of 24 agencies had an established training program in place in comparison to 21 agencies in 2013 (GAO, 2015a).

In regard to monitoring and tracking individual training requirements, it was reported that 16 agencies tracked individual security training status in 2014, in comparison to 19 in 2013 (GAO, 2015a). Finally, in 2014 OMB reported that 24 agencies provided information security training to about 80 percent of personnel, in comparison to 92 percent in the previous year (GAO, 2015a).

The 2015 DoD Cyber Strategy attempts to achieve the requirements set forth in the FISMA 2014, which requires the Defense Department to protect the networks and data from high-risk vulnerabilities (DoD, 2015b). Unknown, high-risk vulnerabilities poses the greatest

threat to DoD networks and systems, as potential adversaries can exploit these systems at any time (DoD, 2015b). A zero-day vulnerability is a security loophole in the software that is unknown to the software maker or to antivirus vendors (Zetter, 2014). Fixing such a vulnerability within the zero-day period requires teamwork across multiple organizations. First, the vendors (i.e., developers) must create and release a patch so that the organizations can remedy the situation in a timely manner. Second, the program managers and CECOM SEC must ensure the software patch is quickly tested, integrated, and delivered to the end-users. Finally, the SASMOs must quickly install the software patch on the system to prevent any further exploitation from adversaries.

The DoD Cyber Strategy points out that the "DoD Chief Information Officer (CIO) will lead an effort to implement an automated patch management capability to distribute software and configuration patches to mitigate known, major vulnerabilities on DoD networks and systems against threats" (DoD, 2015b, p. 20). In accordance with the Army Cyber Command Operations Order 2011-051, "Vulnerabilities are exploitable weakness in software that provide an adversary with an opportunity to compromise the confidentiality, integrity, and/or availability of an Information System" ("Army Small Business," 2015, p. 25). To combat any potential compromise to the network, DoD collaborated with Small Business Innovation Research (SBIR) to develop a viable solution that could be implemented across all the Services.

On August 28, 2015, the DoD (2015a), in collaboration with the SBIR, released a solicitation for "Continuous IAVA Mitigation & Remote Client Support for Tactical Systems." As written within the solicitation, "the objective is to receive a solution on the development of a patch management system capable of providing automated and continuous Information Assurance (IA) patches for fielded, tactical systems, while providing a remote capability for

auditing and assessing system vulnerabilities" (DoD, 2015a). This solicitation helps accelerate the delivery of software patches across all agencies in the DoD domain.

The primary document that addresses the software patch management process is AR 25-2 (Department of the Army, 2009). As mentioned earlier, software patches are periodic fixes that are installed onto the system to correct errors and sometimes enhance functionality of software (Harhai, 2007, p. 6). These patches are required to correct security problems and vulnerabilities on computers. As the life-cycle manager for the systems, the program managers must ensure all computers, including handheld devices, have the latest system security patches to reduce system security vulnerabilities.

According to a 2014 Operational Test and Evaluation (OT&E) annual report, the DoD Director of Operational Test and Evaluation Michael Gilmore stated, "Now and in the future, cybersecurity threats will arguably be some of the most dangerous threats our defense systems face" (Selinger, 2015, p. iii). The OT&E annual report mentioned that the DoD is taking the necessary steps to protect the network; however, many vulnerabilities remain and many more are expected to emerge. Sternstein (2011) reported that software security incidents at Federal agencies spiked to 650 percent, from 5,503 in 2006 to 41,776 in 2010, jeopardizing the information residing on the Government systems.

Program managers realize the majority of a program's cost falls under the sustainment phase. The acquisition community suggests a "70:30 cost ratio with respect to operation and sustainment acquisition of an average weapon system" (Jones, White, Ryan, & Ritschel, 2014, p. 442). According to a document titled *Open Technology Development Lessons Learned and Best Practices for Military Software* (Scott, Wheeler, Lucas, & Herz, 2011), a project is not finished once the capability is transferred to the end-user. In fact, the article continues by stating

that “the operations and maintenance phase of software is characterized by constant changes in the codebase, for any number of reasons: Information Technology (IT) infrastructure changes, hardware changes, software bug fixes, updates and changes, bandwidth and updates in warfighter needs” (Scott et al., 2011, p. 31).

Steve Mills and Rob Goldsmith (2014) emphasized that the “Program Managers (PMs) have the daunting responsibility to minimize cybersecurity vulnerabilities in their systems against current and future cybersecurity” (pp. 41–42). These authors continue to address the importance of prevention in order to operate effectively on the battlefield. Cybersecurity not only addresses hardware and software, but firmware assurance as well.

In regard to the software and firmware assurance, two primary organizations are responsible for releasing the necessary software patches to the tactical system. These two organizations are the PMOs and the CECOM SEC. The PMOs are primarily responsible for managing the software releases for systems that have yet to transition into the sustainment phase. For PMOs, software patches are released under the category of Post-Deployment Software Support (PDSS). Once the program has successfully transitioned the system to sustainment, the SEC is responsible for all aspects of the system maintenance. Software patches released by SEC are commonly referred to as Post-Production Software Support (PPSS). The only difference between PDSS and PPSS is the agency responsible for releasing the software patch. Figure 2 displays the types of software releases within the DoDI 5000.2 acquisition framework.

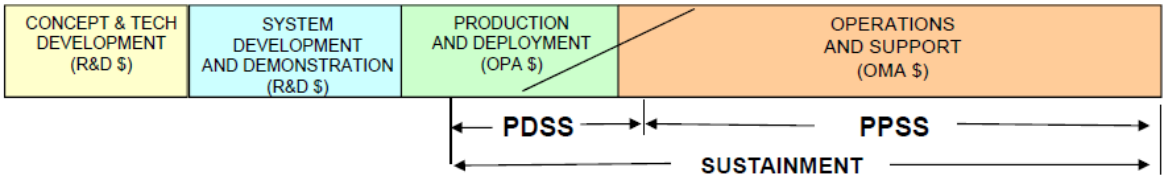


Figure 2 – Types of Software Releases
(Gutleber, 2015)

The frequency of formal software patch releases varies by agency. Typically, they occur on a monthly, quarterly, semi-annual, or annual basis (Scott et al., 2011). In order to reduce security threats to the network, DoD's objective is to reduce the release times to a zero-day patching cycle. One approach for reaching a zero-day patch cycle time is to accelerate the steps within the Information Assurance Vulnerability Management (IAVM).

Information Assurance Vulnerability Management Process

The IAVM process is a disciplined approach for the DoD and other Federal agencies to monitor and control cyber-security risks. AR 25-2 described the IAVM process as "a proactive methodology of maintaining, patching and updating systems before notification or exploitation" (Department of the Army, 2009, p. 44). The DoD (2015c) further explained that the "IAVM process provides positive control over the vulnerability notification process for DoD Network assets" (p. 85). As part of the IAVM process, agencies must acknowledge the receipt of an IAVM message and establish an implementation date. In accordance with AR 25-2, there are four phases of the IAVM process (Department of the Army, 2009, p. 44):

1. Vulnerability identification, dissemination, and acknowledgement
2. Application of measures to affected systems to bring them into compliance
3. Compliance reporting
4. Compliance verification

For the first phase, vulnerability identification, the software flaws or vulnerabilities are initially submitted into the National Vulnerability Database at the National Institute of Standards and Technology. At this point, the vulnerability enters the DoD reporting process starting with United States Cyber Command (USCYBERCOM). Once the vulnerability information is entered, USCYBERCOM notifies their subordinate commands via an alert, bulletin, or a technical tip. In accordance with AR 25-2, IAVAs are the most severe of the three types of notification, and they require acknowledgment from the subordinate agencies.

To help reduce software vulnerabilities and to accelerate the software patching process, Network Enterprise Technology Command (NETCOM)/9th Signal Command Army (SC[A]) published an implementation memorandum for Army Enterprise Desktop Standardization (U.S. Army Enterprise Systems Technology Activity, 2007). This memorandum identified minimum hardware, operating systems, applications, and configuration necessary to establish baselines for personal computer desktop systems for use throughout the Army. The creation of one baseline assists the NEC system administrators to push software patches and other necessary updates to all the systems residing on the garrison network. However, this memorandum does not extend to the software baseline sustained by PMOs/SECs.

AR 25-2 states that PMOs are responsible for addressing corrective actions under their control. As part of the corrective action, PMOs should document compliance using a Scorecard and Plan of Action and Milestone (POA&M). The POA&M documents a temporary workaround until a viable solution can be found. In the meantime, the system and the network continue to be vulnerable to exploitation by adversaries.

Once an IAVA patch is released from a third-party vendor, Army Cyber Command processes it in their system. Subsequently, they release it in parallel to NETCOM/9th SC(A) and

to the United States Army Intelligence and Security Command. NETCOM/9th SC(A) provides notification to the NECs, which are located at each of the major garrison installations. Both the garrison and tactical network fall under the responsibility of NETCOM/9th SC(A). These two networks are "LandWarNet." The primary nontactical network is managed by the garrison NEC. The second network is used extensively in the battlefield and is often referred to as the tactical network. The garrison network is managed by the NEC, while the SASMO community manages the tactical Internet (Department of the Army, 2013).

The SASMO is responsible for "ensuring that all tactical systems are patched in accordance with PM software baseline guidance" (Department of the Army, 2013, p. 3-10). Furthermore, it requires any tactical systems residing on the NEC to be placed on a separate off-line network. This means any tactical system that connects to the NEC's network will be quarantined from the other nontactical office automation systems. This separation enables the NEC to continually patch and monitor their systems without sacrificing the network. For tactical systems residing on the VSAT network, the SASMO is responsible for updating the system, and the SASMO is required to maintain inspection logs annotating the system's name, location, and patches applied to the system (Department of the Army, 2013, p. 64).

Applying IAVA patches may adversely impact the system. As a mitigation plan, the PM ought to test and integrate the patches for interoperability concerns before they distribute the software patches to the end-users. Depending on the type of IAVA severity and the number of patches, a great deal of time may be needed to test and integrate the patch. Some patches may take as little as a few hours, while others may take weeks or months.

Most IAVA patches are added to the Army Knowledge Online database on a monthly basis. For systems that are unable to connect to the database, the PM/CECOM SEC distributes a

CD/DVD on a quarterly basis. In an effort to meet the DoD objective of a zero-day patch cycle, the Army must find alternative ways to accelerate the release rate of IAVA patches to the end-users.

Networks

The Army has two sustainment network environments—the tactical network using Combat Service Support (CSS) VSATs and the garrison network managed by the NEC. The ATP 4-0.6 (Department of the Army, 2013) defines the mission of the SASMO and serves as a guide for SASMO management of the tactical systems and the network. The SASMO is responsible for managing the CSS VSAT along with the tactical information systems. The CSS VSATs are portable satellites managed by Defense-Wide Transmission Systems; they provide data and voice communications connectivity in support of contingency and sustainment missions. These VSATs are employed to support tactical information systems and other C4ISR systems. Figure 3 shows a typical VSAT network diagram with the associated tactical systems connected to it. Although the figure is not very legible, its purpose is not to provide the details, but to show the vast number of heterogeneous systems connected to the network. Each system has a unique and separate software baseline configuration.

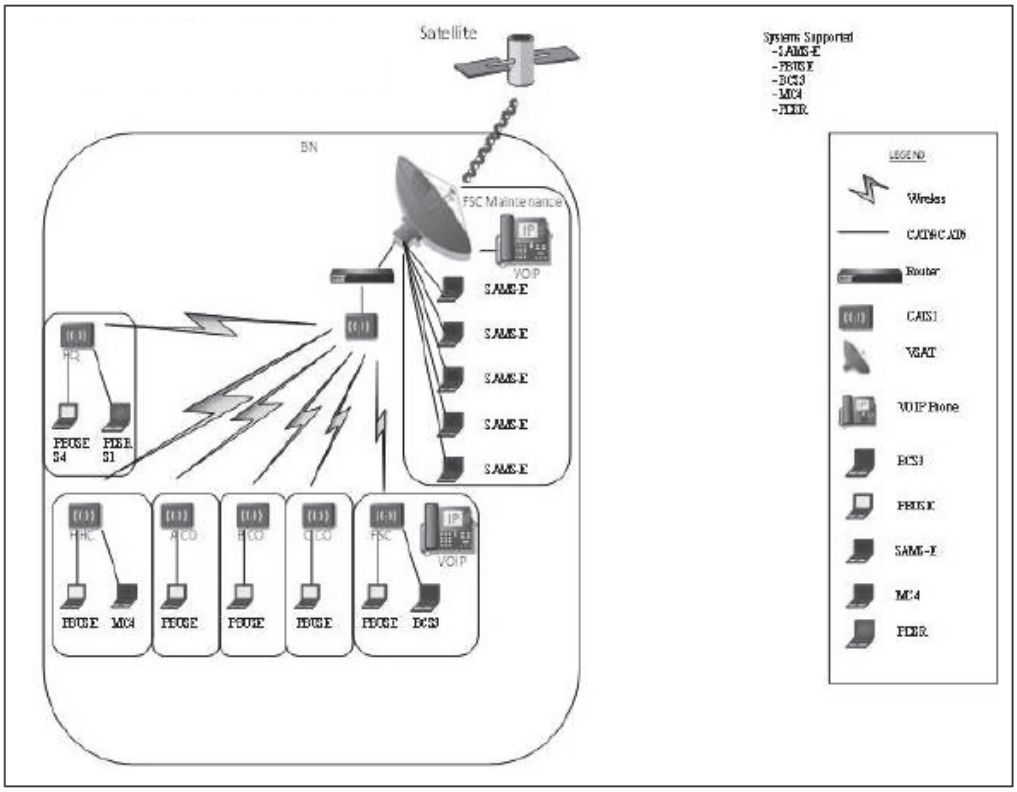


Figure 3 – VSAT Network Diagram
(Source: Department of the Army, 2013)

The NECs' mission is to provide, protect, and defend LandWarNet operations. NECs are located at every major military installation. In simple terms, the NEC manages the Army's standard office computers on the garrison network.

Computers residing on the garrison network can be updated quickly due to the fact that they have a standardized baseline of hardware and software. However, tactical computers using the CSS VSAT network must be updated manually due to the unique software applications. If VSATs are not patched with the latest software security patches, then they could be vulnerable to external cyberattacks. A report generated by security researchers at IntelCrawler, a Los-Angeles-based cyber intelligence company, indicated there are approximately 3 million VSAT terminals in the world (Paganini, 2014). Of these active VSATs, more than two-thirds are being utilized by

the Government to transmit information (Storm, 2014). The Army employs many of these VSATS during a bi-annual Network Integration Evaluation (NIE) exercise that focuses on securing the tactical Internet. With the increased threats to networks, Pomerleau (2015) believes, "Network defense is job No.1 for the Army."

The SASMO has the authority to allow or deny access of devices on the network to ensure that the entire network—software, hardware, and users—are in compliance with ARs 25-1 and 25-2. In addition, the SASMO is responsible for the physical security of the network. The SASMO generates and maintains a Tactical Network Diagram (Figure 3) for all the systems residing on the VSAT network. The NEC is not responsible for managing the PM's software baseline. In addition, the NEC is not required to connect the tactical system to their garrison network. In other words, the SASMO works independently from the garrison NEC. Basically, each organization is responsible for managing its own network.

According to Cohen (2009), one challenge noticed by a deployed SASMO was how he was assigned to Network Operations instead of being assigned to a company as required by the Modified Table of Equipment. This organizational realignment had a major impact on the SASMO community, because they spent their time working and supporting the tasks of the Network Operations section and not supporting the direct unit with the tactical systems. As a result, the tactical systems were not properly patched, leaving the network vulnerable for exploitation.

Commercial-Off-the-Shelf Software Vulnerabilities

In early 1997, DoD acquisition emphasized the maximum use of commercial-off-the-shelf (COTS) items (DiMarco, 2000). Although there were benefits to inserting COTS into the DoDI 5000.2 acquisition framework, there were unforeseen consequences as well. One

unforeseen impact of incorporating COTS into the field was the additional workload pushed onto organizations, which now had to monitor and release continuously, across the network, software patches of commercial software products. As addressed earlier, the PMOs and CECOM SEC are responsible for testing, integrating, and releasing software patches to the end-users. This section provides an historical overview of the software vulnerabilities over the last 25 years, giving a better appreciation of the workload requirement by the PMOs and CECOM SEC to release software patches once vulnerabilities are reported to USCYBERCOM.

The following charts display vulnerabilities of commonly used third-party software. It's important to note that there are many tactical systems that employ a combination of COTS and Government-only software products. Ensuring that both these software products work hand-in-hand is critical. According to Florian (2015), approximately 7,038 new security vulnerabilities were reported in 2014 (Figure 4), an average of 19 vulnerabilities per day. The data came from the National Vulnerability Database, which provides an extensive list of third-party software security vulnerabilities.

Year	# of vulnerabilities
2010	4,258
2011	3,532
2012	4,347
2013	4,794
2014	7,038

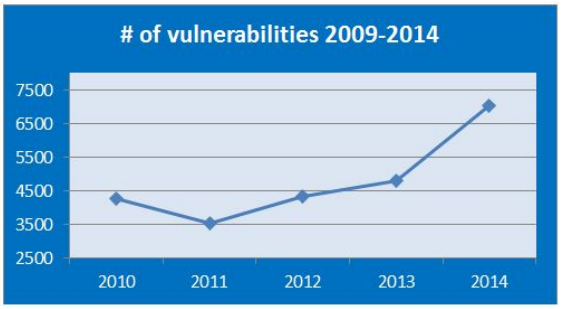


Figure 4 – Vulnerabilities 5-Year Trend
(Source: Florian, 2015)

A more comprehensive look of software vulnerabilities—over the last 25 years—can be seen in a research report generated by Yves Younan (2013), a senior research engineer for Sourcefire. Figure 5 gives a snapshot of these vulnerabilities, starting in 1988 and ending with

2012. It's worth noting that the number of vulnerabilities in 2000, when the DoD started pushing the use of COTS, was 1,020 compared to the 5,281 in 2012. This quantity is staggering, because it means that the PMOs/CECOM SEC must test and integrate all these software patches before releasing them to the SASMO community.

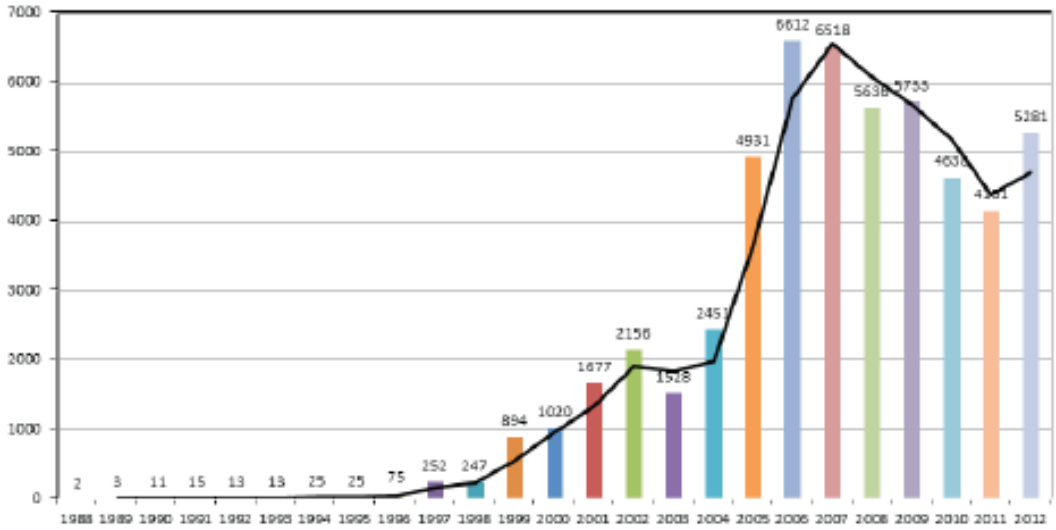


Figure 5 – Vulnerabilities by Year
(Source: Younan, 2013)

Figure 6 provides a percentage break-out of vulnerabilities by product type. Florian (2015) reported that over 83 percent of the reported vulnerabilities were found in the software applications, while 13 percent and 4 percent were found in operating systems and hardware devices, respectively.

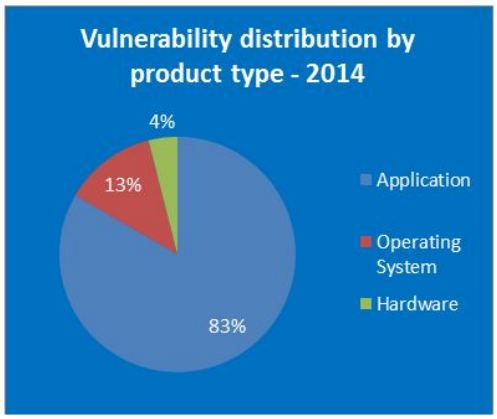


Figure 6 – Vulnerability by Product Type
(Source: Florian, 2015)

Figure 7 (Florian, 2015) compares the number of high-severity vulnerabilities to the total number of vulnerabilities reported from 2010 to 2014. It shows that the number of high-severity vulnerabilities has slowly risen over the last 3 years. The upward trend is alarming, because most of the high-severity vulnerabilities require immediate attention. This means the PMOs and CECOM SEC must prioritize their resources to address the high-severity issues ahead of the more abundant vulnerabilities. No matter what software vulnerability the PMOs and CECOM SEC tackles, there will be an inevitable delay in the release of a software patch to the SASMO community.

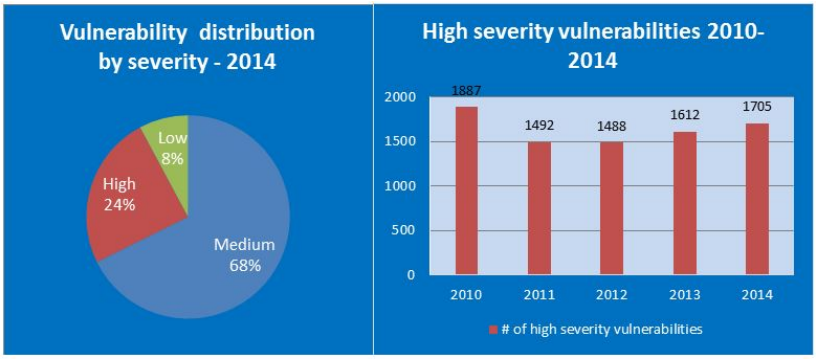


Figure 7 – High-Severity Vulnerabilities 2010–2014
(Source: Florian, 2015)

Chapter 3 – Research Methodology

Research Hypothesis

It is hypothesized the SASMOs cannot maintain system IAVA compliance on tactical systems using the current Army IAVA Software Patch Management Process due to the frequent releases of third-party software patches.

Research Design

The purpose of this study is to explore the software patch management process of the systems on the tactical Internet. Based on the literature review as well as the survey responses, the research captures information on the notification, distribution, and installation process. The intent is to review the feedback from the respondents to determine any significant gaps in their responses regarding the software patch process. If any significant response gaps exist, the data may be used as indicators to determine whether any necessary procedures, tools, and/or resources are required to streamline the software update process.

Research Process

As mentioned in Chapter 1, this research used qualitative and quantitative information. The literature review as well as the survey tool, called SurveyMonkey, focused on three key organizations—the PMO, SEC, and the SASMO community. The research focused on the software patch management process from the perspectives of the PMO, CECOM SEC, and the SASMO community. Notification, dissemination, and installation were the key categories of the process that were examined. The research did not focus on the development, testing, and integration process within the PMO or SEC.

The literature review included peer-review articles, service-related publication, DoD/Department of the Army regulations, policy, and doctrine. Other information was extracted

from GAO reports and publications. Given the sensitive nature of the topic, data was limited to information readily available on the Internet. All information within this research paper is unclassified.

The survey tool used for this research was SurveyMonkey. Questions were posed to three major organizations: PMO, SEC, and the SASMO community. The questions covered some basic demographic data to obtain rank and position of respondent to ensure responses were from reputable personnel in relevant positions. The questions focused on the software update process in regard to notification, distribution, installation, and reporting. The survey was developed to capture responses from key positions with each organization.

The survey not only captured the software patch management process, it captured training certification levels of the respondents and personnel shortages within the SASMO community to determine whether experience and personnel shortages may affect the time required to install the software patch on the systems. Finally, the survey asked individuals within each organization to grade themselves on their process. This self-assessment would be compared to the feedback from the SASMO community. The disparity, if any, between these self-assessment responses may lead to awareness that an issue exists in the software update process.

Data Collection

The survey comprised 33 questions. Depending on the respondents, the questions varied. For example, the SASMO community had 22 questions, whereas the PM and SEC had 11 questions. The initial questions captured their position along with their experience level and certification level. The remaining questions focused on the specific software patch process within each of their respective organizations. The final question focused on implementing a

tactical system Command Cyber Readiness Inspection similar to the DISA NEC. A complete list of questions can be found in Appendix A.

The analysis from the survey examined the software patch process from the perspective of the three organizations. The conclusion and recommendation are addressed in Chapter 5.

Bias and Error

The most significant bias in this research paper is the insertion of personal experience with the software patch management process. The type of literature review found and reported in this paper can be a source of bias. Much of literature review focused on the negative aspect of the software management process primarily due to the information readily available in various reports and articles. A potential error that may exist is the possibility that new policy and procedures may be available, but unknown to the researcher at the time the literature review was conducted. Other possible threats to validity include selection and unique programs. To account for selection and unique program features, the survey covered all the programs supported by SASMO support structure.

Validity of Responses

Any subjective data collected by way of comments requires an additional investigation or clarification using email to determine the validity of data. As a result, certain biases may be contributed to the knowledge and expert opinion of the researcher. The survey questionnaire was distributed to the SASMO community in all three Army components (i.e., Active, National Guard, and Reserve), CECOM SEC, and Product Management Offices.

Reliability of Responses

The survey questions were provided to Combined Arms Support Command (CASCOM) headquarters, which manages the SASMOs across the Active, Reserve, and National Guard

components. Before the official release of the survey, the questions were provided to CASCOM and PMO/SEC for a quality review to ensure the questions were not vague or ambiguous in meaning. The survey responders have access to the information needed to respond to all survey questions.

Chapter 4 – Findings

Collected Data

Preceding this chapter, the literature and IAVM process outlined the responsibilities of the various organizations and the overlapping relationship among them for third-party software patch management. The purpose of this section is to analyze and explain the challenges with implementing a software patch management plan from the viewpoint of each organization. The hypothesis is the SASMO community cannot maintain system IAVA compliance on tactical systems using the current Army IAVA Software Patch Management Process due to the frequent releases of third-party software patches.

This chapter focuses on two key areas. The first section analyzes the timeframe required to test, integrate, and distribute the software patch from the perspective of the PMO and CECOM SEC. The second section analyzes the challenges in regard to the notification, receipt of software patches from the PMO/CECOM SEC, and the installation process from the viewpoint of the SASMO community.

A SASMO is similar to the Greek myth of Sisyphus, who was the king of Ephyra. In this story, King Sisyphus was punished by being forced to roll an immense boulder up a hill, only to watch it roll back down just prior to reaching the top, repeating this action for eternity. This story is similar to the life of a SASMO in regard to software patch management. Regardless of how hard the SASMO works to install software patches on their systems, they feel like Sisyphus pushing the boulder from the bottom of the hill every time a new software patch is released.

So how does the PMO/CECOM SEC and the SASMO work collaboratively to shift the patch installation date closer to the actual disclosure and patch release date as shown in the Figure 8?

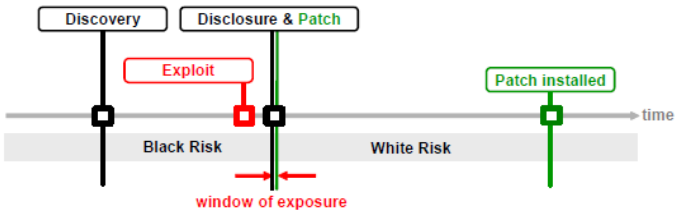


Figure 8 – 0-Day Patch Cycle
(Source: Frie, Tellenbach, & Plattner, 2008)

The major challenge the PMOs and CECOM SEC face is to keep up with the testing, integration, and dissemination of numerous third-party software patches in order for the SASMOs to protect the network from intrusion. Although this section does not address all the intricacies involved in the PM/CECOM SEC testing and integration schedule, it does highlight a generic timeline of their software patch management process. Based on my experience within a program management office, the PMOs release IAVAs on a quarterly basis. This doesn't imply that the SASMOs receive the most up-to-date IAVAs. In fact, these quarterly IAVA releases from the PMO/CECOM SEC are usually 2 to 3 months behind the most current third-party release schedule. The reason behind the gap stems from the PMO's IAVA management process, which establishes a cut-off date for accepting new IAVA updates to their testing and integration baseline. As part of the PM's and CECOM SECs' software configuration process, the cut-off date to accept any additional software into the next software baseline marks the official start date for formalized testing and integration. Once the SASMOs receive the patches, the installation process typically takes them a few months to complete. Therefore, many systems are 4 to 5 months behind the original release schedule. This is one indicator that the SASMOs cannot achieve the DoD CIO objective for zero-day patch management.

A second factor to consider in the software release timeline is the PMO/CECOM SEC notification and dissemination process. Currently, AR 25-2 indicates the PM and CECOM SEC

will notify and provide the unit with the IAVA patches. Based on my experience, the PMO typically gives a bulk notification via email based on their last distribution list, which does not guarantee a valid and reliable notification list. In parallel to crafting a notification email, the PMO commences the media duplication process, and subsequently distributes the media to various units based on their last known SASMO shipping address. The DVD duplication process takes approximately a week to produce about 200 IAVA DVD packages. The current number of Army units in need of the IAVA updates is approximately 2,400. Thus, it could take about 10 weeks before the last batch of IAVA DVDs are ready for shipment. Based on this process, the SASMO is already months behind applying the original software patches.

From a connectivity perspective, the SASMOs have the technology and the bandwidth in garrison to download any size of software. If the PMO wants to expedite the delivery process, then they need to post all IAVA patches to a centralized database that all SASMOs can access. Currently, based on my research, the Army doesn't have a mechanism in place to automate patch delivery by proactively pushing updates and security patches to their customers to protect their system. This approach would not only reduce the time in the notification and dissemination process, it would significantly reduce shipping and duplication costs. If the connectivity and technology are readily available for the SASMO community to employ, then there is a possibility to reduce significantly the patching release and installation timeline.

Most of the tactical systems supported by the SASMO community are COTS-based hardware using COTS-based applications, such as Windows Operating System and other Microsoft Office products. To appreciate the complexity and vulnerability of modern software, one must understand that Microsoft Windows 8 has over 50 million lines of code. Steve McConnell (2004) indicated that the industry standard for software defects is about 20 to 50

defects per 1,000 lines of code. This equates to approximately 2.5 million potential defects in the software for possible exploitation. This is one of the reasons behind the frequent patch releases by Microsoft. Couple Microsoft's software releases with numerous other third-party patches, and the software patch management process becomes very difficult to monitor and manage for both the PMO/CECOM SEC and the SASMO community.

According to a survey on Windows patching, conducted by Network World (2011), system administrators reported three challenges with software patching. First, rebooting servers after updates is highly disliked due to the associated system/network downtime. The second concern was the lack of personnel to perform system upgrades across the network. The third concern, but not the least, was the exorbitant amount of time required to test the patch against other software applications before the patch could be installed onto the system. Based on this article, several system administrators acknowledge that a major dilemma with patching the Windows Operating System is the need to reboot the server, which often cannot be accomplished during the day due to the organization's mission. A time assessment was performed in early 2009 by a Microsoft team, which reported the time required to upgrade from Vista SP1 to Windows 7 ranged from 30 minutes to 1,220 minutes (Protalinski, 2009). Network World (2011) explained the great range in the time required to update a system:

> Custom software came in as the main reason it would take more than 24 hours to test and deploy patches. Yet not far behind was the lack of manpower to roll out critical patches; testing less-important patches ranked lower in priorities. And very close behind was the fact that people frequently find that Microsoft's patches cause issues with software and resolving those issues often took more than 24 hours.

Based on the number of software vulnerabilities reported by Younan (2013), which averages approximately 19 per day, program managers and CECOM SEC would have to hire a significant amount of personnel to keep up with the daily level of effort. Even if the PMO and CECOM SEC could test and integrate all the daily released patches within a 24-hour period, the delivery of the patch would have to be expedited to the field. Based on the literature review, PMOs and CECOM SEC deliver these patches via DVD/CD because their size makes it impossible to push them through the limited bandwidth on the VSAT network. By the time the software media are duplicated and shipped to the various units, the SASMO would still have to coordinate with the command group to install the patch. The shipment-to-installation timeline could take a week to a month, even longer if the unit is not properly staffed with a SASMO. Lindstrom (2016) provides a common equation to determine the cost of patch management:
(Hours x Rate x Systems) + (Patch Failure% x (Hours x Rate x Systems)) = Cost to Patch

Imagine a SASMO being injected in the commercial market. In this scenario, the SASMO would be considered an entry-level system administer who gets paid at an hourly rate. For this scenario, the SASMO will receive approximately $30/hour to support 400 systems. The cost to perform the patch would be $12,000 per patch. If a standard 5 percent of the patches fail, requiring an average of two hours for recover time, that's 20 systems at $60 (two hours)—which equals $1,200. Therefore, the total patch time is 440 hours at a cost of $13,200. Now, recall the DoD CIO guidance to move to a zero-day patch cycle. The SASMO community would have to perform this activity every day based on the daily average of 19 vulnerabilities being reported by third-party vendors. To understand the impact across the force, imagine this process being implemented across the entire SASMO community, which is estimated to be about 2,000

personnel. Given the cost and level of effort across the force, achieving a zero-day patch objective is unrealistic.

As Dorado and Richards (2011) indicated, “the problem with updating the system is due to an array of new systems, each having its own distinct configuration requirement.” They continued to explain that many SASMOs come into a unit typically knowing little about the unit’s operation, and there are no management tools fielded with any systems that the SASMO supports (Dorado & Richards). This story relates closely to the findings in previous GAO reports in that many Federal agencies lack sound configuration management controls. Even though 24 Federal agencies had software configuration plans, 17 of them were significantly deficient in implementing software patches. One could argue that even if software patches were readily available for immediate installation, many agencies, including the SASMO community, would have difficulty maintaining their systems because they do not know how many assets are in their inventory and the current software configuration of each system.

A similar configuration/inventory management problem was documented by Ryan (2012), who described the common frustration in the SASMO community about not having a clear picture of all the communication assets within their units. Ryan indicated that it is no longer enough to know how many radios, antennas, computers, and printers are in a unit. The SASMO is responsible for tracking a myriad of other technical information for IAVA compliance, such as software version, Media Access Control and Internet Protocol address, Lightweight Directory Interchange Format, interoperability, compatibility, classification, antivirus and domain status, and the support chain of each asset. One approach to assist the SASMO community is to use a standard automated monitoring and management tool to capture all software-related issues for each system. A centralized asset management database could assist the SASMO community by

sending out periodic vulnerability status reports for each system under their responsibility. Ideally, this proposed system should be closely interoperable with the Army Property Book Accountability System to ensure all assets are accounted for and maintained across the battlefield. Currently, SASMOs do not have a common enterprise system to capture system information.

Shortage of personnel to support simultaneous operations and new logistics automation systems was addressed by Sawyer, Petty, and Shaw (2010). They addressed the insufficient number of SASMOs to support the various units in a split-based operation while in Operation Iraqi Freedom. Another reference point showing lack of personnel in the SASMO section is documented in Frazier (2011). Frazier reported that many of the SASMOs are forced to support the mission at 20 to 30 percent of their full complement. She advised the senior SASMO to address the personnel issue with the command by showing how the lack of personnel affects the mission. Another concern regarding the personnel shortfall is the time it takes to update all the systems on the network with reduced personnel. As indicated previously, many of the IAVA patches require manual updates. The SASMOs need to find the appropriate time to perform the updates so as to avoid affecting the commander's mission. The fewer people to perform the updates, the more network downtime will occur. Now, imagine the frustration the commanders have when the SASMO has to constantly apply patches to the system due to the high frequency of third-party software releases. Even if software patches were readily available, sometime the commander's direct the SASMO to install the patches at a given time (e.g., once a month) to reduce mission impact.

The DoD CIO realized the importance of developing and incorporating measures to help reduce network vulnerabilities brought on by commercial software vulnerabilities. DoD's

(2015b) Cyber Security Strategy emphasized the importance of incorporating additional cybersecurity assessments into the various Army training events at the National Training Center and the Joint Readiness Training Center. Prior to the DoD Cyber Security Strategy, some units were conducting limited cybersecurity exercises. However, Neely (2013) and Ryan (2012) only indicated that the unit performed network protection, which may or may not include software patch management. Neither article mentioned whether software patch management was specifically performed during these training exercises. Furthermore, many units do not touch their systems once they enter the training event. The standard procedure is to update the systems to the latest software version before and after the training event.

Although the Army's software patch management process described in AR 25-2 appears to work for computers on the garrison network with standard hardware and software configurations, it doesn't appear that it can work with tactical systems that have many hardware configurations with many software configuration baselines. One more concern regarding the software patch management process is the increased quantity of software patches being reported on a daily basis. Each of these software vulnerabilities needs to be individually tested and integrated into the software baseline before it can be released to the field. The time to perform these activities can be days, weeks, or months depending on the severity of the vulnerability and the complexity of the program's software baseline. Having a known vulnerability on the network for any extended period of time gives our adversaries time to exploit the system and cause disruption in the unit's operation. If the Army wants to protect their network from software vulnerabilities, then the entire software patch management process needs to be reviewed and modified to expedite the release of software patches.

In summary, there appears to be similar third-party software patch management challenges facing the PMO/CECOM SEC and the SASMO community as well as other Federal agencies. Although most agencies report to have well-documented configuration control management plans, the prevalent issue is implementation of their software patch management plan. All parties have a shared responsibility in the patch management process, from the PMO/CECOM SEC to test, integrate, and disseminate the patch, to the SASMO community to install the software patch onto the information systems. The reoccurring theme within this chapter is that each organization has challenges with software patch management. These include, but are not limited to, the time required to test and integrate the third-party patches into software baselines; the notification process, personnel, and training required to release patches; the mode of delivery of patches; configuration and asset management accountability; and the lack standard enterprise monitoring and patching applications.

Chapter 5 – Interpretation

The purpose of this chapter is to provide an interpretation of my findings based on the evidence within this literature review and additional evidence-based information from the previous chapter. Subsequent to the interpretation, I will provide recommendations that may be employed for future research on software patch management process. In the last section I will recap the limitations of this study.

Conclusions

My hypothesis is that the SASMO community cannot maintain system IAVA compliance on tactical systems using the current Army IAVA Software Patch Management Process due to the frequent releases of third-party software patches. In addition to the hypothesis, two research questions were proposed to address the acceleration of the deployment and installation of the software patches from each organization. Based on the literature review and other evidence-based information, the findings support my hypothesis. Even though the SASMO community could accelerate the software-patching installation timeline from the PMO/CECOM SEC software patch release date, the accelerated schedule is predicated on personnel taking a more active role in software patch management and the incorporation of new technology to monitor and manage the systems better. At this time, it appears the SASMO community is unable to keep up with the frequent delivery of third-party patches using their current delivery and installation processes.

DoD CIO guidance has emphasized software security management across all agencies, but software patching of tactical IT systems remains an ongoing challenge. Based on the literature review, the underlying problem is not the lack of guidance and policy, or “what” needs to be done. The problem is “how” to accomplish it. The underlying problem is there doesn’t

appear to be a central standard enterprise solution for software patch management, as evidenced by DoD's recent solicitation to industry for such an enterprise solution. Thus, I conclude that guidance is secondary to personnel monitoring and managing the process. The software patch management process is only as good as the personnel actively managing the process.

Technology also plays a significant role in the process. To implement a successful patch management plan, personnel need to be properly trained in their respective roles at the levels of proficiency appropriate to address rapidly changing technologies. Personnel not attending security awareness training may miss the opportunity to obtain basic understanding of information security requirements to protect their systems. Agencies not requiring personnel to take the specialized training, or not monitoring their compliance, are hindering their professional development.

Recommendations

This section offers three recommendation for further research on patch management: a standard enterprise patch management tool, cloud-based management, and Government-developed software. The first recommendation is to incorporate a standard enterprise software patch management tool that can be used across all organizations. This tool would manage all the assets and track the software configurations of each system. It would be able to generate reports for the system administrators to improve tracking and monitoring of system compliance. In addition, this software tool could provide update notifications to the command about their systems. One implication of this tool is the need to obtain buy-in from the various stakeholders; for this tool to work effectively, all stakeholders need to endorse the process. Without the support from the tactical commander, no process will be successful. The other part of this recommendation is to have patch docking stations accessible across the installation. Once the

computers are synched in the docking station, the computer system would communicate with the server to apply the necessary updates. Any updates to the system would be logged into the previously mentioned software management tool.

A second recommendation to assist the SASMOs with achieving a zero-day patching is to transition the tactical information system applications to a cloud-based operation. In this situation, the units will be issued a standard notebook without any applications. All the applications would reside on an application server. Since there aren't any applications on the computer, there is little possibility for software vulnerabilities. This approach would resolve many issues related to software patching. First, the SASMO would only have to patch the applications on the server and not each individual notebook. This would significantly reduce the hours required to perform patch management. Patching could be performed in hours instead of days or weeks. Instead of deploying a team of SASMOs to the field, it would require only one SASMO to perform the software patch on the server.

An additional benefit to cloud-base management is the positive impact on mission readiness. With the current process, the SASMO must schedule a time with the unit commander to patch the systems. It is reasonable to assume that at certain times a commander may mandate the system administrator to patch the systems at a later time so as not to affect their daily operations. Therefore, the SASMO is forced to work on the information systems after normal work hours, or in the worst case, the system would have to be patched during normal operational hours due to the criticality of the patch. However, if the applications reside on the server, then the system administrators can install the software patches without affecting daily operations. A significant concern with this approach would be the bandwidth connectivity. The unit would need to have sufficient network connectivity to access the applications without impacting their

mission. Currently, the available of VSAT bandwidth sharing is a major concern across the force. The implication from this recommendation is that additional funding would have to be allocated to the VSAT program office to support the increased bandwidth requirement.

The final recommendation is to develop Government-only software. The PMO would develop and manage the software code for their respective systems. There are many implications with this recommendation, ranging from staffing actions, additional acquisition regulatory requirements, and funding to support the additional level of effort. The advantage of this recommendation is that it enables full access to and control of the software code in order to make any necessary software configuration changes to correct a security vulnerability.

Limitations of the Study

Due to the time constraint and the survey-based policy change, chapters 4 and 5 were significantly modified to reflect an evidence-based approach from a survey-based approach. As a result of the change in policy, a more extensive literature review revealed no additional literature. However, some resources addressed some Federal agencies that had roles and responsibilities that could be closely associated with those of the SASMO community. Although the duties and responsibilities may be similar, the environment and the systems in which the system administrators operate are very different, even unique.

References

Army small business inovation research proposal submission instructions. (2015). Retrieved from http://www.acq.osd.mil/osbp/sbir/solicitations/sbir20153/army153.pdf

Cohen, R. (2009). Adaptability is critical to NETOPS in battle. *Army Communicator, 34*(2), 17.

Darcey, R. F. (2003). *Effective patch managment is critical to mitigating software vulnerabilities* (GAO-03-1138T). Washington, DC: General Accounting Office.

Department of the Army. (2009). *Information assurance* (Army Regulation 25-2). Washington, DC: Author.

Department of the Army. (2013). *Techniques for sustainment information systems support* (Army Techniques Publication 4-0.6). Washington, DC: Author.

Department of the Army. (2014). *Army acquisition procedures* (Army Regulation Pamphlet 70-3). Washington, DC: Author.

Department of Defense. (2015a). *Continuous IAVA mitigation & remote client support for tactical systems*. Retrieved from https://www.sbir.gov/sbirsearch/detail/825619

Department of Defense. (2015b). *Cyber security strategy.* Retrieved from http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Department of Defense. (2015c). *Information assurance workforce improvement program* (8570.01-M). Washington, DC: Author.

DiMarco, K. A. (2000). *Commercial item acquisition: Considerations and lessons learned.* Retrieved from www.acq.osd.mil/dpap/Docs/cotsreport.pdf

Dorado, J., & Richards, J. (2011, Spring). Signal life in the logistics lane. *Army Communicator*, 60–62. Retrieved from http://signal.army.mil/armyComArchive/2011/Vol36/No1/2011Vol36No1Sub15.pdf

Federal Information Security Management Act, 116 Stat. 2946 (2002).

Federal Information Security Modernization Act, 128 Stat. 3073 (2014).

Florian, C. (2015). *Most vulnerable operating systems and applications in 2014.* Retrieved from http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/

Frazier, N. (2011). *Embracing the SASMO mission*. Retrieved from http://www.thefreelibrary.com/Embracing+the+SASMO+mission.-a0279891000

Frie, S., Tellenbach, B., & Plattner, B. (2008). *0-Day patch exposing vendors (in)security performance*. Retrieved from https://www.blackhat.com/.../bh...08/.../bh-eu-08-frei-WP.pdf

Government Accountability Office. (2004). *Information security: Continued action needed to improve software patch management* (GAO-04-706). Washington, DC: Author.

Government Accountability Office. (2011). *Weakness continues amid new federal efforts to implement requirements* (GAO-12-137). Washington, DC: Author.

Government Accountability Office. (2014). *Information security: VA needs to address identified vulnerabililities* (GAO-15-117). Washington, DC: Author.

Government Acccountability Office. (2015a). *Agencies need to correct weaknesses and fully implement security programs* (GAO-15-714). Washington, DC: Author.

Government Accountability Office. (2015b). *Information security: IRS needs to continue improving controls over financial and taxpayer data* (GAO-15-337). Washington, DC: Author.

Gutleber, M. (2015). *Department of the Army budget process and the challenges ahead for estimating software support.* Retrieved from http://www.psmsc.com/UG2012/Presentations/07%20-%20Gutleber%20-%20CECOM%20SEC%20presentation%20on%20ppss%20to%20software%20working%20group.pdf

Harhai, S. (2007). Conquering computer updates and upgrades. *Family Advocate, 29*(4), 6–7.

Jones, G., White, E., Ryan, E., & Ritschel, J. (2014). Investigation into the ratio of operating and support costs to life-cycle costs for DoD weapon systems. *Defense Acquisition Research Journal, 21*(1), 442–464.j

Lindstrom, P. (2004). *A patch in time: Considering automated patch management*. Retrieved from http://searchsecurity.techtarget.com/A-Patch-in-Time-Considering-automated-patch-management-solutions

McConnell, S. (2004). *Code complete: A practical handbook of software construction* (2nd ed.). Redmond, Washington: Microsoft Press.

Meister, T. (2015). *Idaho National Guard soldiers first to defeat cyber-attacks at National Training Center*. Retrieved from https://www.dvidshub.net/news/175860/idaho-national-guard-soldiers-first-defeat-cyber-attacks-national-training-center

Mills, S., & Goldsmith, R. (2014). Cybersecurity challenges for program managers. *Defense AT&L, 43*(5),41–43. Retrieved from http://www.dau.mil/publications/DefenseATL/DATLFiles/Sep-Oct2014/Mills_Goldsmith.pdf

Neely, J. (2013). Sustainment Automation Support Management Office operations at JRTC. *Army Sustainment, 45*(1), 52–53. Retrieved from http://www.alu.army.mil/alog/issues/JanFeb13/Sustainment_Automation_Support.html#.

Network World. (2011). *Patching windows is a major time sink for IT departments*. Retrieved from http://www.networkworld.com/article/2229227/microsoft-subnet/patching-windows-is-a-major-time-sink-for-it-departments.html

Paganini, P. (2014). *VSAT terminals are opened for targeted cyber attacks*. Retrieved from http://pcsupport.about.com/od/termsp/g/patch-fix.htm

Pomerleau, M. (2015). *Cyber defense front and center at NIE*. Retrieved from https://gcn.com/Articles/2015/10/06/Cyber-defense-NIE.aspx

Protalinski, E. (2009). *Microsoft: Windows 7 upgrade can take nearly a day (updated x2).* Retrieved from http://arstechnica.com/information-technology/2009/09/microsoft-upgrade-to-windows-7-can-take-up-to-a-day/

Ryan, M. (2012, Winter). National Training Center: Success tips for battalion signal officers. *Army Communicator*, 33–38. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA577754

Sawyer, A., Petty, R., & Shaw, J. (2010). Improvement strategies for logistics automation support. *Army Sustainment, 42*(6). Retrieved from http://www.alu.army.mil/alog/issues/NovDec10/improv_strategies.html

Scott, J., Wheeler, D., Lucas, M., & Herz, J. (2011). *Open technology development (OTD): Lessons learned & best practices for military software.* Retrieved from http://dodcio.defense.gov/Portals/0/Documents/FOSS/OTD-lessons-learned-military-signed.pdf

Selinger, M. (2015). *DoD systems still vulnerable to cyber threats*. Retrieved from https://news.clearancejobs.com/2015/01/31/dod-systems-still-vulnerable-cyber-threats-report-says/

Souppaya, M., & Scarfone, K. (2013). *Guide to enterprise patch management technologies* (NIST Special Publications 800-40 Rev. 3). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

Sternstein, A. (2011). *GAO: Federal network security breaches spike 650 percent.* Retrieved from http://m.nextgov.com/cybersecurity/2011/10/gao-federal-network-security-breaches-spike-650-percent/49874/

Storm, D. (2014). *Hackers exploit SCADA holes to take full control of critical infrastructure*. Retrieved from http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html

U.S. Army Enterprise Systems Technology Activity. (2007). NETCOM/9th ASC technical authority (TA) implementation memorandum (2003-005d). Fort Huachuca, AZ: Author. Retrieved from http://network6.net/n/netcom-9th-asc-technical-authority-(ta)-implementation-memorandum-w16358

Younan, Y. (2013). *25 years of vulnerabiltieis: 1988–2012*. Retrieved from http://www.servnet.inf.br/pdf/sourcefire_historico_vulnerabilidades_entre_1988_e_2012.pdf

Zetter, K. (2014). *Hacker lexicon: What is Zero Day?* Retrieved from http://wired.com/2014/11/what-is-a-zero-day/

Glossary of Acronyms and Terms

AR.....Army Regulation

ATP.....Army Technique Publication

C4ISR.....Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

CASCOM.....Combined Arms Support Command

CCRI.....cyber command readiness inspection

CECOM.....Communications Electronics Command

CIO.....chief information officer

COTS.....commercial off the shelf

CSS.....Combat Service Support

DISA.....Defense Information Security Agency

DoD.....Department of Defense

DoDI.....Department of Defense Instruction

FISMA.....Federal Information Security Management Act

GAO.....General Accounting Office/Government Accountability Office

IAVA.....Information Assurance Vulnerability Alert

IAVM.....Information Assurance Vulnerability Management

NEC.....Network Enterprise Center

NETCOM.....Network Enterprise Command

OMB.....Office of Management and Budget

OT&E.....Operational Test and Evaluation

PDSS.....Post-Deployment Software Support

PM.....Program Manager/Product Manager

PMO.....Program Management Office

POA&M.....Plan of Action & Milestones

PPSS.....Post-Production Software Support

SASMO.....Sustainment Automation System Management Office

SBIR.....Small Business Innovation Research

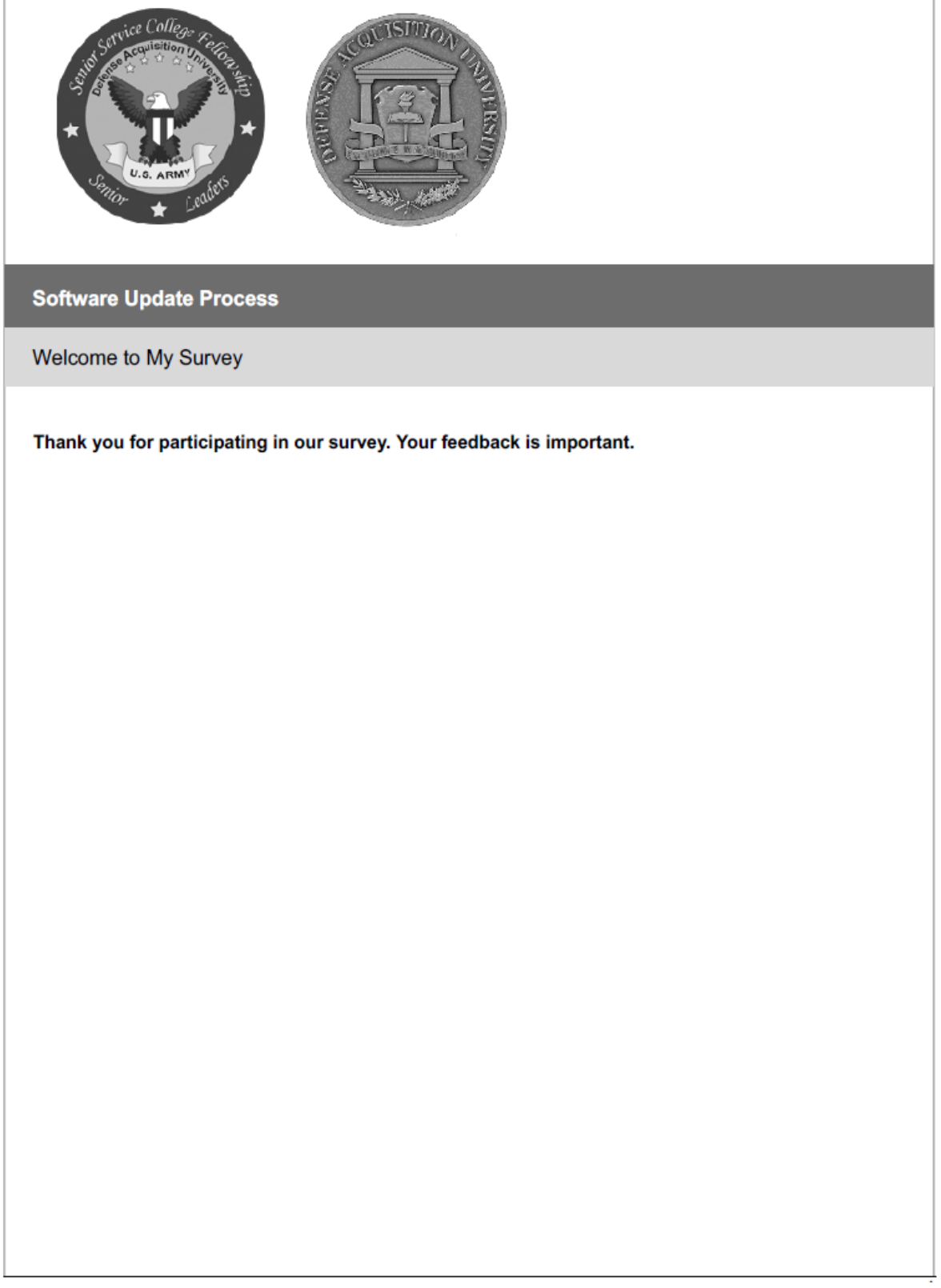
SC(A).....Signal Command (Army)

SEC.....Software Engineering Center

USCYBERCOM……United States Cyber Command

VSAT.....Very Small Aperture Terminal

Appendix A – Survey Tool



Software Update Process

Informed Consent Agreement

INFORMED CONSENT AGREEMENT

The purpose of this research survey is to assess and project the experience and generational mix of our future Army acquisition workforce. Your input is very important.

1. INFORMED CONSENT AGREEMENT:

As an adult 18 years of age or older, I agree to participate in this research about assessing the effectiveness of the software update process of tactical information systems. This survey is being conducted to support research efforts being performed by Benjamin Pryor, a student of the Army Senior Service College Fellowship Program of the Defense Acquisition University.

I understand that my participation is entirely voluntary; I can withdraw my consent at any time. By agreeing to participate in this study, I indicate that I understand the following:

1. The purpose of the research is to assess the software patch management process of tactical information systems. Should I choose to participate in the survey, I am aware that my feedback will be consolidated with other participants and the outcome maybe briefed to Army leadership allowing them to potentially take action on my recommendations.

2. If I choose to participate in this research, I will be asked to complete an online questionnaire. The questionnaire will include items relating to the software patch management process of tactical information systems from the perspective of the Program/Product Office, Software Enterprise Center (SEC), and Sustainment Automation Support Management Officers (SASMO). The questionnaire will take approximately [10-15] minutes to complete.

3. There is no incentive for participation.

4. All items in the questionnaire are important for analysis and my data input will be more meaningful if all questions are answered. However, I do not have to answer any that I prefer not to answer. I can discontinue my participation at any time without penalty by exiting out of the survey.

5. This research will not expose me you to any discomfort or stress beyond that which might normally occur during a typical day. There are no right or wrong answers; thus, I need not be stressed about finding a correct answer.

6. There are no known risks associated with my participating in this study.

7. Data collected will be handled in a confidential manner. The data collected will remain anonymous.

8. The purpose of this research has been explained and my participation is entirely voluntary.

9. I understand that the research entails no known risks and by completing this survey, I am agreeing to participate in this research.

END OF INFORMED CONSENT

* 1. I have read the Informed Consent Agreement and will participate voluntarily.

- ◯ Yes
- ◯ No

Software Update Process

Organization

* 2. Please select your organization:

- ◯ PEO/PM/PdM
- ◯ Software Engineer Center (SEC)
- ◯ Sustainment Automation Support Management Officer (SASMO)

Software Update Process

Sustainment Automation Support Management Officer (SASMO)

* 3. What component do you fall under?

- ◯ Active Army (COMPO 1)
- ◯ Army National Guard (COMPO 2)
- ◯ Army Reserve (COMPO 3)

* 4. What is your MOS?

* 5. How many years of experience to you have as a SASMO? (round to the closest year)

- ◯ 1-5 years
- ◯ 6-10 years
- ◯ 11+ years

* 6. What's your level of expertise with the software updating process of the following systems?

	Not at all familar	Slightly Familiar	Moderately familiar	Very Familiar	Extremely familiar
AIT	○	○	○	○	○
BCS3	○	○	○	○	○
CAISI	○	○	○	○	○
MC4	○	○	○	○	○
MROCS	○	○	○	○	○
MTS	○	○	○	○	○
PBUSE	○	○	○	○	○
SAAS-MOD	○	○	○	○	○
SAMS-E	○	○	○	○	○
SARSS1	○	○	○	○	○
TC-AIMS II	○	○	○	○	○
VSAT	○	○	○	○	○

* 7. Upon receipt of the software update, how much time elapses before it is installed onto these systems?

	Daily	Weekly	Monthly	Greater than Monthly	N/A
AIT	○	○	○	○	○
BCS3	○	○	○	○	○
CAISI	○	○	○	○	○
MC4	○	○	○	○	○
MROCS	○	○	○	○	○
MTS	○	○	○	○	○
PBUSE	○	○	○	○	○
SAAS-MOD	○	○	○	○	○
SAMS-E	○	○	○	○	○
SARSS1	○	○	○	○	○
TC-AIMS II	○	○	○	○	○
VSAT	○	○	○	○	○

* 8. Once the system has been updated, how often do you notify the respective PMs/SEC?

	Daily	Weekly	Monthly	Greater than Monthly	Never
Program/Product Management Office	◯	◯	◯	◯	◯
Software Engineer Center	◯	◯	◯	◯	◯

* 9. Do you currently possess the necessary certifications per Techniques for Sustainment Information Systems Support (ATP 4-0.6)?

- ◯ Yes
- ◯ No
- ◯ Don't know

* 10. In response to previous question, what certification level are you?

- ◯ Level 1
- ◯ Level 2

* 11. Rate yourself based on your expertise to perform software updating on the systems within your Area of Operation.

Very poor	Poor	Fair	Good	Excellent
◯	◯	◯	◯	◯

* 12. Based on your current MTOE authorization, do you have any personnel (SASMO) shortages?

- ◯ Yes
- ◯ No
- ◯ Don't know

* 13. On a scale of 1-5 (1= no impact to 5= significantly impacts), how do personnel shortages impact your timeline to patch the systems?

1	2	3	4	5
◯	◯	◯	◯	◯

* 14. Do you have the necessary software updating accessories to perform software update?

- ◯ Yes
- ◯ No

* 15. Do you maintain a detailed list by serial number, software version, and last software update of the systems within your Area of Responsibility?

- ◯ Yes
- ◯ No

* 16. Do you have a written standard operating procedure (SOP) on software updating management?

- ◯ Yes
- ◯ No
- ◯ Don't know

* 17. Do you have a software management tool to monitor systems on your network?

- ◯ Yes
- ◯ No

* 18. Is there value added to implement a Command Cyber Readiness Inspection (CCRI) for systems residing on the tactical internet?

- ◯ Yes
- ◯ No

* 19. Who notifies you of a system update? (select all that apply)

- ☐ Program/Product Office
- ☐ S-6/G6
- ☐ Other SASMOs (community blog)
- ☐ Software Enterprise Center (SEC)
- ☐ Other (please specify)

* 20. Do you have a software application that installs software updates?

- ◯ Yes
- ◯ No

21. Do you have working knowledge of the documents listed below? (select all that apply)

- [ ] ATP 4-0.6 Techniques for Sustainment Information Systems Support
- [ ] Cybersecurity DoDI 8510.01
- [ ] ATP 4-93 Sustainment Brigade
- [ ] DoD 5400.11-R Department of Defense Privacy Program
- [ ] DoD 6025.18-R Department of Defense Health Information Privacy Regulation
- [ ] DoD 8580.02-R Department of Defense Health Information Security Regulation

* 22. How likely are the systems to be vulnerable to security issues due to latency in their updating processes?

Not at all likely	Slightly likely	Moderately likely	Very likely	Completely likely
○	○	○	○	○

Software Update Process

Program/Product Managers and Software Enterprise Centers

* 23. What position are you serving in?

- ◯ PM or deputy PM
- ◯ Cybersecurity Officer
- ◯ Information Systems Security Officer (ISSO)
- ◯ Life-cycle Logistics
- ◯ Software Engineer Center (SEC)

* 24. What DAWIA certifications do you hold?

	Level 1	Level 2	Level 3	N/A
Program Management	◯	◯	◯	◯
Engineering	◯	◯	◯	◯
Life-Cycle Logistics	◯	◯	◯	◯
Information Technology	◯	◯	◯	◯
Science and Technology	◯	◯	◯	◯

* 25. Over the last 12 months, how many software updates has your organization released?

- ◯ 1-10
- ◯ 11-15
- ◯ 16+

* 26. How do you distribute your software updates? (Select all that apply)

- [ ] Internet (downloadable)
- [ ] DVDs
- [ ] CTR support personnel (PM-managed)
- [ ] Other (please specify)

* 27. Who do you notify of software updates? (Select all that apply)

- [ ] Commander
- [ ] S1/G1
- [ ] S2/G2
- [ ] S3/G3
- [ ] S4/G4
- [ ] S6/G6
- [ ] SASMO
- [ ] Logistics Assistance Representative (LAR)
- [ ] Other (please specify)

* 28. How accurate is your SASMO contact distribution list?

0-30%	31%-50%	51%-69%	70%-89%	90%-100%
○	○	○	○	○

* 29. How often is your SASMO distribution list updated?

Weekly	Daily	Quarterly	Annually	Never
○	○	○	○	○

30. How do you verify that your SASMO distribution list is current?

* 31. How do you notify the people people on the SAMSO distribution list? (Select all that apply)

- [ ] Email (direct)
- [ ] Email (general distribution; bulk spam)
- [ ] phone call
- [ ] website (posting)
- [ ] You don't notify them
- [ ] Other (please specify)

* 32. Does your organization utilize an universal, centralized database that displays "all" available software updates for your respective system?

- ◯ Yes
- ◯ No
- ◯ Don't know

* 33. Does your organization have a written post-deployment software support / post-production software support plan (PDSS/PPSS)?

- ◯ Yes
- ◯ No
- ◯ Don't know

* 34. Based on timeliness, how do you rate your program on providing the following items?

	Very Poor	Poor	Fair	Good	Excellent
Notification	◯	◯	◯	◯	◯
Delivery of Software	◯	◯	◯	◯	◯

* 35. In general, how would you rate the SASMOs within each COMPO on the timely installing of software patches?

	Don't know	Poor	Fair	Good	Excellent
Active Army (COMPO 1)	◯	◯	◯	◯	◯
Army National Guard (COMPO 2)	◯	◯	◯	◯	◯
Army Reserve (COMPO 3)	◯	◯	◯	◯	◯

* 36. Should a Command Cyber Readiness Inspection (CCRI) be implemented for systems on the tactical internet?

- ◯ Yes
- ◯ No

Software Update Process

Final Thoughts

37. Do you have any comments?

Software Update Process

Survey Completion

Thank you for your time. Your input is very valuable.